

CLAIMS

1. A secret key generating method for generating secret keys of an entity at a plurality of key generating agencies, respectively, comprising the steps of:

dividing identification information of the entity into a plurality of blocks so as to obtain divided identification information for each of the key generating agencies;

selecting a plurality of bits of any order for each of the key generating agencies from a predetermined sequence of a plurality of bits so as to set a hash value consisting of a plurality of bits for each of the key generating agencies;

and

generating the secret keys of the entity by using the divided identification information and the hash values.

2. An encryption method for encrypting a plaintext to be transmitted from a first entity to a second entity, comprising the steps of:

generating secret keys of the first entity by using respective divided identification information obtained by dividing identification information of the first entity into a plurality of blocks and hash values, each consisting of a plurality of bits, set for a plurality of key generating agencies, respectively;

generating a common key by using components

corresponding to the second entity, contained in the generated secret keys; and

encrypting the plaintext into a ciphertext by using the generated common key,

wherein the hash values are set for the key generating agencies, respectively, by selecting a plurality of bits of any order for each of the key generating agencies from a predetermined sequence of a plurality of bits.

GOVERNMENT OF CANADA - 1985

3. A cryptographic communication method for communicating information by a ciphertext between first and second entities, comprising the steps of:

sending from each of a plurality of key generating agencies to each of the first and second entities a secret key generated by using each of divided identification information obtained by dividing identification information of each entity into a plurality of blocks and a hash value which consists of a plurality of bits and is set for each of the key generating agencies;

at the first entity, generating a first common key by using components corresponding to the second entity as a destination of ciphertext, contained in the secret keys of the first entity sent from the key generating agencies, respectively;

at the first entity, encrypting a plaintext into a

ciphertext by using the generated first common key and transmitting the ciphertext to the second entity;

at the second entity, generating a second common key identical with the first common key by using components corresponding to the first entity, contained in the secret keys of the second entity sent from the key generating agencies, respectively; and

at the second entity, decrypting the transmitted ciphertext into a plaintext by using the generated second common key,

wherein the hash value is set for each of the key generating agencies, by selecting a plurality of bits of any order for each of the key generating agencies from a predetermined sequence of a plurality of bits.

4. A cryptographic communication system which permits a plurality of entities to mutually perform an encryption process for encrypting a plaintext as information to be transmitted into a ciphertext and a decryption process for decrypting the transmitted ciphertext into the original plaintext, comprising:

a plurality of key generating agencies, each of which generates a secret key of each entity by using each of divided identification information obtained by dividing identification information of each entity into a plurality of

blocks and a hash value which consists of a plurality of bits and is set for each of the key generating agencies and sends the generated secret key to each entity; and

a plurality of entities, each of which generates a common key for use in the encryption process and decryption process by using components corresponding to an entity to be communicated with, contained in its own secret keys sent from the key generating agencies, respectively,

wherein the hash value is set for each of the key generating agencies, by selecting a plurality of bits of any order for each of the key generating agencies from a predetermined sequence of a plurality of bits.

5. The cryptographic communication system as set forth in claim 4,

wherein, when a new key generating agency is added to a plurality of existing key generating agencies, a hash value is set for the new key generating agency by selecting a plurality of bits of any order from an original hash-value sequence consisting of a sequence of hash values set for the existing key generating agencies.

6. A computer memory product having computer readable program code means for causing a computer to

generate secret keys of an entity at a plurality of key generating agencies, respectively, said computer readable program code means comprising:

program code means for causing the computer to select a plurality of bits of any order for each of the key generating agencies from a predetermined sequence of a plurality of bits so as to set a hash value consisting of a plurality of bits for each of the key generating agencies; and

program code means for causing the computer to generate the secret key of the entity for each of the key generating agencies by using the hash value and divided identification information for each of the key generating agencies obtained by dividing identification information of the entity into a plurality of blocks.

7. A computer data signal embodied in a carrier wave for transmitting a program, the program being configured to cause a computer to generate secret keys of an entity at a plurality of key generating agencies, respectively, comprising:

a code segment for causing the computer to select a plurality of bits of any order for each of the key generating agencies from a predetermined sequence of a plurality of bits so as to set a hash value consisting of a plurality of bits

for each of the key generating agencies; and
a code segment for causing the computer to generate
the secret key of the entity for each of the key generating
agencies by using the hash value and divided identification
information for each of the key generating agencies
obtained by dividing identification information of the entity
into a plurality of blocks.